## Insert for Developer's Statement of Work

### 2. Applicable Documents

The documents listed in this section are applicable to this project. The Contractor shall protect the confidentiality of FAA Protection Profiles, Security Targets, TOEs, and assurance evidence IAW the FAA orders and policy memorandums cited below.

### 2.1 Government Documents

- ACP-300-00-001, FAA Policy Memorandum, Safeguarding and Control of Sensitive Security Information (SSI), January 30, 2002.
- ATS-SEC-99-001, FAA Policy Memorandum, Safeguarding and Control of Classified and Sensitive Information, September 23, 1999.
- FAA Order 1370.82, Information Systems Security Program, June 2000 (or latest version).
- FAA Order 1370.83, Internet Access Points, February 2001.
- FAA Order 1600.2, Safeguarding Controls and Procedures for Classified National Security Information and Sensitive Unclassified Information.
- FAA Order 1600.69, FAA Facilities Security Management Program.
- FAA Order 1600.6, FAA Physical Security Management Program.
- FAA Order 1600.1D, Personnel Security Program.
- FAA Order 1600.72, Contractor and Industrial Security Program, April 4, 2001.
- FAA Information System Security Enhancement Program Handbook, version 3 (or most current version).
- NIST SP 800-37, Guidelines for the Security Certification and Accreditation of Federal IT Systems, June 2003 (or later version).
- FAA GCNSS CIN Common Information Base Protection Profile, version 1.0, 12 January 2004
- FAA GCNSS CIN Common Transport Network Protection Profile, version 1.0, 12 January 2004

### 2.2 Non-Government Documents

- ISO/IEC 15408-1 Information Technology - Security Techniques - Evaluation Criteria for IT, Security - Part 1: General Model, December 1999.
- ISO/IEC 15408-2 Information Technology - Security Techniques - Evaluation Criteria for IT Security - Part 2: Security Functional Requirements, December 1999.

- ISO/IEC 15408-3 Information Technology - Security Techniques - Evaluation Criteria for IT Security - Part 3: Security Assurance Requirements, December 1999.
- The Common Methodology for IT Security Evaluation (CEM), Parts 1 and 2, including draft supplements for Maintenance of Assurance (AMA) and Vulnerability Analysis and Penetration Testing (AVA).

## 4. Task Requirements

### 4.1 Task 1 -- Information Security

#### 4.1.1 Security Functional Requirements (SFRs)

The contractor shall implement all of the security functional requirements identified in the Protection Profiles cited in subsection 2.1 of this SOW. The contractor shall implement all of the security functional requirements listed in Section 5 of the Protection Profiles cited in subsection 2.1 of this SOW, so that:

(a) All of the security objectives stated in Section 4 of the Protection Profile cited in subsection 2.1 of this SOW are met.
(b) All of the Section 3 assumptions are adhered to, threats are countered, and organizational security policies are enforced. In particular, the contractor should pay attention to the assigned risk mitigation priorities.
(c) They are consistent and compatible with the operational environment described in Section 2 of the Protection Profile cited in subsection 2.1 of this SOW.
(d) They satisfy the strength of function (SOF) requirements stated in Section 1 of the Protection Profile cited in subsection 2.1 of this SOW.

#### 4.1.2 Security Assurance Requirements (SARs)

The Contractor shall perform all of the security assurance requirements identified in the Protection Profiles cited in subsection 2.1 of this SOW. The contractor shall perform all the developer action elements and produce all of the content and presentation of evidence elements, stated in ISO/IEC 15408 Part 3 for the security assurance requirements. The contractor shall perform these activities and produce this evidence to ensure that the stated EAL is achieved.

The contractor shall utilize the documentation and evidence produced in response to the security assurance requirements as input to the FAA C&A process. In particular, the Contractor shall use this information to satisfy the C&A subtasks in NIST SP 800-37. The contractor shall prepare the security assurance documentation/evidence with this dual use in mind.

## 5. Deliverables

### 5.1 Security Deliverables

The contractor shall prepare all information security deliverables in accordance with the specified Data Item Description (DID). The contractor should note that the content requirements are derived from the ISO/IEC 15408-3 content and presentation of evidence requirements for each SAR.

All security sensitive deliverables shall be protected IAW the FAA orders and policy memorandum cited in Section 2.1 of this SOW.

All evaluation reports and other documentation produced under this contract remains the property of the FAA and may not be disclosed without prior written consent from the Contracting Officer.